PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-345752
(43)Date of publication of application : 05.12.2003

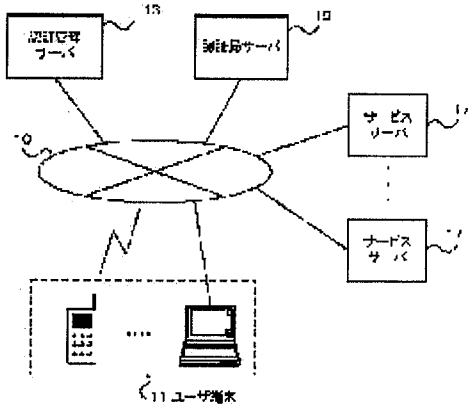
(51)Int.Cl. G06F 15/00
G06F 17/60
H04L 9/32

(21)Application number : 2002-151144
(22)Date of filing : 24.05.2002

(71)Applicant : NTT DATA CORP
(72)Inventor : HIROTA KAZUYA
TANAKA ICHIRO
KUSUDA TETSUYA
MIYATA KOJI
YOKOYAMA SHIGETOSHI

(54) AUTHENTICATION MANAGEMENT SERVER AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To protect the privacy of a user by enabling the user himself/herself to control contents of user information released for account registration.
SOLUTION: An authentication management server 13 acquires from a user terminal 11 information inputted by the user as the user information to be released to a service server 17 in registering an account in a service. Then, the authentication management server 13 requests an authentication station server 15 to issue an electronic certificate based on the information inputted by the user, acquires the electronic certificate (persona ID) and registers the electronic certificate in a database. The authentication management server 13 uses the acquired electronic certificate (persona ID) and performs account registration for the service designated by the user.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－345752
（P2003－345752A）
(43)公開日　平成15年12月5日(2003.12.5)

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｂ	５Ｂ０８５
	17/60	１４０	17/60	１４０	５Ｊ１０４
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ 9/00	６７５Ｚ	

審査請求　有　　請求項の数５　　ＯＬ　（全 17 頁）

(21)出願番号　特願2002－151144(P2002－151144)

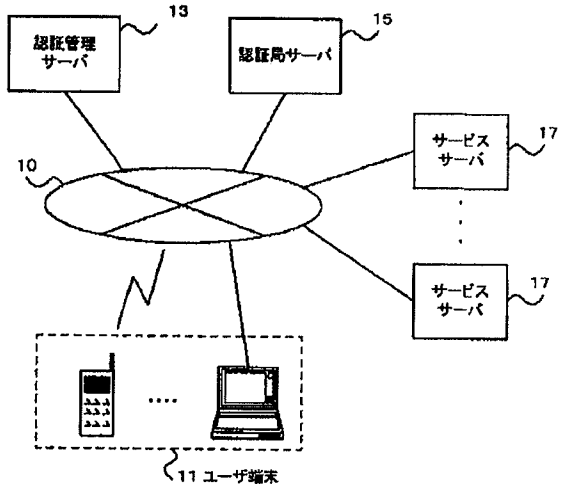
(22)出願日　平成14年５月24日(2002.5.24)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　廣田　和也
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　田中　一郎
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100095407
弁理士　木村　満

最終頁に続く

(54)【発明の名称】　認証管理サーバ及びプログラム

(57)【要約】
【課題】　アカウント登録のために開示するユーザ情報の内容をユーザ自身がコントロールすることで、ユーザのプライバシーを保護する。
【解決手段】　認証管理サーバ１３は、サービスへのアカウント登録時にサービスサーバ１７に開示するユーザ情報としてユーザが入力した情報をユーザ端末１１から取得する。そして、認証管理サーバ１３は、ユーザより入力された情報に基づく電子証明書の発行を認証局サーバ１５に要求して電子証明書（ペルソナＩＤ）を取得して、データベースに登録する。そして、認証管理サーバ１３は、取得した電子証明書（ペルソナＩＤ）を用いてユーザにより指定されたサービスへのアカウント登録を行う。



【特許請求の範囲】
【請求項１】複数のサービス提供サーバに接続可能であって、ユーザ端末からの要求に応じてサービス提供サーバへのログインを代行する認証管理サーバであって、
ユーザにより指定されたサービスの情報をユーザ端末から取得する手段と、
前記ユーザにより指定されたサービスへのアカウント登録時にサービス提供サーバに開示するユーザ情報としてユーザが入力した情報を前記ユーザ端末から取得する手段と、
前記ユーザ情報に基づく電子証明書の発行を認証機関に要求して取得し、データベースに登録する手段と、
前記取得した電子証明書を用いて前記ユーザにより指定されたサービスへのアカウント登録を行う手段と、
を備えることを特徴とする認証管理サーバ。
【請求項２】ユーザにより指定された使用対象の電子証明書の情報をユーザ端末から受信し、　ユーザにより指定された利用対象のサービスの情報を前記ユーザ端末から受信し、
前記指定された使用対象の電子証明書を前記データベースから読み出し、当該電子証明書を用いて、前記指定された利用対象のサービスへログインする、
ことを特徴とする請求項１に記載の認証管理サーバ。
【請求項３】ユーザにより指定されたサービスについて、アカウント登録に必要なユーザ情報をサービス提供サーバに問い合わせる手段と、
前記問い合わせ結果に基づき、前記ユーザについて前記サービスへのアカウント登録に用いる電子証明書を取得する取得手段と、
前記取得した電子証明書を用いて前記サービスへのアカウント登録を行う手段と、
を備えることを特徴とする請求項２に記載の認証管理サーバ。
【請求項４】前記取得手段は、
前記問い合わせ結果が示すアカウント登録に必要なユーザ情報に適合する電子証明書が前記ユーザについて登録されているか否かを前記データベースを参照して判別し、
前記適合する電子証明書が登録されていると判別した場合、当該電子証明書を前記アカウント登録に用いるものとし、
前記適合する電子証明書が登録されていないと判別した場合、前記アカウント登録に必要なユーザ情報をユーザ端末を介して取得し、取得したユーザ情報に基づく電子証明書の発行を認証機関に要求し、発行された電子証明書を前記アカウント登録に用いるものとする、
ことを特徴とする請求項３に記載の認証管理サーバ。
【請求項５】コンピュータを、複数のサービス提供サーバに接続可能であってユーザ端末からの要求に応じてサービス提供サーバへのログインを代行する認証管理サーバとして機能させるためのプログラムであって、
ユーザにより指定されたサービスの情報をユーザ端末から受信する手段、
前記ユーザにより指定されたサービスへのアカウント登録時にサービス提供サーバに開示するユーザ情報としてユーザが入力した情報を前記ユーザ端末から受信する受付手段、
前記ユーザ情報に基づく電子証明書の発行を認証機関に要求して取得し、データベースに登録する手段、
前記取得した電子証明書を用いて前記ユーザにより指定されたサービスへのアカウント登録を行う手段、
として機能させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、複数のサービス提供元に対するユーザ認証を代行する認証管理サーバ等に関する。
【０００２】
【従来の技術】従来、ログイン時における本人確認手段として、認証機関により発行された電子証明書を用いた認証が一般的に行われている。例えばユーザが複数のサービス提供元によるサービスを利用するようなシステムでは、ユーザは各サービス提供元に対してそれぞれ電子証明書を提示して認証を受ける必要がある。この場合、ユーザは複数のサービス提供元に対して同じ証明書を使用するか、または、サービス毎に異なる証明書を使用することとなる。
【０００３】
【発明が解決しようとする課題】上記のようなシステムでは、通常、サービス利用に必要な個人情報（ユーザ情報）が電子証明書に含まれるが、複数のサービス提供元に対して同じ証明書を使用する場合、あるサービス提供元に対してはユーザが開示したくない情報まで提供してしまう可能性があり、ユーザのプライバシーが保護されない虞がある。また、サービス毎に異なる電子証明書を使用する場合、ユーザは利用するサービス毎に電子証明書を取得しなければならず煩雑であった。
【０００４】この発明は、上記実状に鑑みてなされたものであり、ユーザのプライバシーを保護することができる認証管理サーバ等を提供することを目的とする。また、この発明は、ユーザの利便性を向上することができる認証管理サーバ等を提供することを他の目的とする。
【０００５】
【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点に係る認証管理サーバは、複数のサービス提供サーバに接続可能であって、ユーザ端末からの要求に応じてサービス提供サーバへのログインを代行する認証管理サーバであって、ユーザにより指定されたサービスの情報をユーザ端末から取得する手段と、前記ユーザにより指定されたサービスへのアカウン

ト登録時にサービス提供サーバに開示するユーザ情報としてユーザが入力した情報を前記ユーザ端末から取得する手段と、前記ユーザ情報に基づく電子証明書の発行を認証機関に要求して取得し、データベースに登録する手段と、前記取得した電子証明書を用いて前記ユーザにより指定されたサービスへのアカウント登録を行う手段と、を備えることを特徴とする。

【０００６】この発明によれば、アカウント登録のために各サービス提供側へ開示するユーザ情報（氏名、住所、年齢等）の内容をユーザがサービス毎に指定することができるため、自己の情報の開示についてユーザ自身がコントロールすることができ、ユーザのプライバシーを保護することができる。また、各サービスへのアカウント登録や、各サービスに提示する電子証明書の取得・管理を認証管理サーバが行うことにより、ユーザの負荷が軽減され、システムの利便性を向上することができる。

【０００７】ユーザにより指定された使用対象の電子証明書の情報をユーザ端末から受信してもよく、ユーザにより指定された利用対象のサービスの情報を前記ユーザ端末から受信してもよく、前記指定された使用対象の電子証明書を前記データベースから読み出し、当該電子証明書を用いて、前記指定された利用対象のサービスへログインしてもよい。

【０００８】ユーザにより指定されたサービスについて、アカウント登録に必要なユーザ情報をサービス提供サーバに問い合わせる手段と、前記問い合わせ結果に基づき、前記ユーザについて前記サービスへのアカウント登録に用いる電子証明書を取得する取得手段と、前記取得した電子証明書を用いて前記サービスへのアカウント登録を行う手段と、を備えてもよい。これにより、ユーザにとって利便性の高いシステムを実現することができる。

【０００９】前記取得手段は、前記問い合わせ結果が示すアカウント登録に必要なユーザ情報に適合する電子証明書が前記ユーザについて登録されているか否かを前記データベースを参照して判別してもよく、前記適合する電子証明書が登録されていると判別した場合、当該電子証明書を前記アカウント登録に用いるものとしてもよく、前記適合する電子証明書が登録されていないと判別した場合、前記アカウント登録に必要なユーザ情報をユーザ端末を介して取得し、取得したユーザ情報に基づく電子証明書の発行を認証機関に要求し、発行された電子証明書を前記アカウント登録に用いるものとしてもよい。

【００１０】この発明の第２の観点に係るプログラムは、コンピュータを、複数のサービス提供サーバに接続可能であってユーザ端末からの要求に応じてサービス提供サーバへのログインを代行する認証管理サーバとして機能させるためのプログラムであって、ユーザにより指定されたサービスの情報をユーザ端末から受信する手段、前記ユーザにより指定されたサービスへのアカウント登録時にサービス提供サーバに開示するユーザ情報としてユーザが入力した情報を前記ユーザ端末から受信する受付手段、前記ユーザ情報に基づく電子証明書の発行を認証機関に要求して取得し、データベースに登録する手段、前記取得した電子証明書を用いて前記ユーザにより指定されたサービスへのアカウント登録を行う手段、として機能させる。

【００１１】

【発明の実施の形態】以下、本発明の実施の形態に係るユーザ認証システムについて図面を参照して説明する。

【００１２】図１はこの発明の実施の形態に係るユーザ認証システムの構成を示す図である。図示するように、このユーザ認証システムは、ネットワーク１０を介して相互に接続されるユーザ端末１１と、認証管理サーバ１３と、認証局サーバ１５と、サービスサーバ１７と、を備えている。

【００１３】ネットワーク１０は、移動体通信網、電話回線、インターネット等から構成され、ユーザ端末１１と各サーバとの間で情報の送受信を可能とするためのものである。

【００１４】ユーザ端末１１は、携帯端末、携帯電話機、パーソナルコンピュータ等から構成され、ネットワーク１０を介して認証管理サーバ１３等との間で通信を行う。ユーザ端末１１は、図示せぬ記憶部に記憶される動作プログラム等を実行することにより、認証管理サーバ１３を介して各サービスサーバ１７による各種サービスの提供を受けるための処理等を行う。また、ユーザ端末１１は、ＷＥＢページの閲覧、電子メールの送受信等のインターネットに関する機能を有する。

【００１５】また、ユーザ端末１１は、ＳＩＭ（Subscriber Identity Module card）と称されるＩＣカード等の情報記憶媒体が接続可能に構成されている。ＩＣカード等には、ユーザの電子証明書（プライマリＩＤ）、秘密鍵、公開鍵等の情報が記憶可能である。ここで、プライマリＩＤとは、ユーザが認証管理サーバ１３にログインする際に使用される電子証明書であり、ユーザ端末１１がユーザの操作に従って認証局サーバ１５に要求して発行を受ける。このプライマリＩＤはユーザの個人情報（ユーザ情報）等を証明書内容として含み、例えば図２に示すように、ユーザの氏名、住所、年齢等のメイン情報と、ペンネーム、興味分野等の付属情報と、ユーザの公開鍵等を署名対象の情報とする。ユーザは、このプライマリＩＤを用いて認証管理サーバ１３に対してユーザ登録を行う。

【００１６】認証管理サーバ１３は、例えば図３に示すように、制御部１３１と、記憶部１３２と、通信制御部１３３と、を備えるコンピュータ等から構成される。

【００１７】制御部１３１は、記憶部１３２に記憶され

る動作プログラム等を実行することにより、要求処理部１３１ａ、ユーザ認証部１３１ｂ、証明書管理部１３１ｃ、サービスＩＦ（インタフェース）部１３１ｄ、セッション管理部１３１ｅ、暗号処理部１３１ｆ等を論理的に実現する。

【００１８】要求処理部１３１ａは、ユーザ端末１１へ供給する処理画面の生成、ユーザ端末１１からの要求受付等の処理を行う。ユーザ認証部１３１ｂは、ユーザ登録、ログインユーザの認証等の処理を行う。ユーザ登録処理では、ユーザ端末１１からユーザのプライマリＩＤを取得して、記憶部１３２に登録する。また、ログインユーザの認証処理では、ユーザ端末１１から提示されたプライマリＩＤを照合することによりログインユーザの正当性を確認する。

【００１９】証明書管理部１３１ｃは、ユーザがサービスサーバ１７にログインする際に使用する電子証明書（ペルソナＩＤ）の発行・管理に関する処理等を行う。具体的には、ペルソナＩＤの発行に際し、発行対象の証明書の内容をユーザに指定させ、その内容の証明書の発行を認証局サーバ１５に要求し、発行されたペルソナＩＤをユーザ毎に記憶部１３２に記憶する。ペルソナＩＤは、例えば図４に示すように、プライマリＩＤと同様にユーザ情報等を証明書内容として含み、メイン情報と付属情報とユーザの公開鍵等を署名対象の情報とする。ペルソナＩＤのメイン情報は、プライマリＩＤにおけるメイン情報の一部又は全部から構成される。ペルソナＩＤの情報内容はプライマリＩＤの情報内容を包含するように広く設定されてもよく、例えば、プライマリＩＤにおける「年齢：２５歳」という情報をペルソナＩＤにおいて「年齢：１８以上」と設定してもよい。また、付属情報についてはユーザが内容を自由に指定することができ、例えばプライマリＩＤにおける付属情報の内容と異なっていてもよい。

【００２０】サービスＩＦ部１３１ｄは、ユーザが各サービスサーバ１７によるサービスを利用するための処理等を行う。具体的には、ユーザ認証部１３１ｂによるログインユーザの認証完了後、そのユーザについて登録されているペルソナＩＤから使用対象のペルソナＩＤをユーザに選択させる。そして、選択されたペルソナＩＤで利用可能なサービスのリストをユーザに提示し、利用対象のサービスを選択させる。そして、選択されたサービスを提供するサービスサーバ１７に、選択されたペルソナＩＤを用いてログインする。そして、サービスサーバ１７によりペルソナＩＤが認証された場合には、サービスサーバ１７とユーザ端末１１の間で送受信データを仲介することにより、ユーザのサービス利用を可能とする。

【００２１】また、サービスＩＦ部１３１ｄは、ユーザから新規サービスの登録要求を受けた場合には、そのサービス提供元のサービスサーバ１７に対して、ユーザ登録に必要なユーザ情報を問い合わせ、そのユーザの既存のペルソナＩＤでユーザ登録が可能である場合にはユーザ登録を行う。また、既存のペルソナＩＤではユーザ登録ができない場合には、ユーザに必要な情報を入力させ、新たなペルソナＩＤの発行を受けてユーザ登録を行う。

【００２２】セッション管理部１３１ｅは、ユーザのサービス利用時におけるセッション管理等の処理を行い、ユーザ端末１１との通信と、サービスサーバ１７との通信で、使用するセッションキーの変換等を行う。暗号処理部１３１ｆは、電子署名の確認処理やデータの暗号化／復号化処理等を行う。

【００２３】記憶部１３２は、制御部１３１が実行する動作プログラムや、処理に必要な各種のデータを記憶する。また、記憶部１３２は、各ユーザについての所定情報を記憶するユーザＤＢ１３２ａを備える。ユーザＤＢ１３２ａには、例えば、個人情報（氏名、住所、年齢等）、プライマリＩＤ、ペルソナＩＤ、各ペルソナＩＤにより利用可能なサービスの情報等がユーザ毎に記憶される。

【００２４】通信制御部１３３は、ネットワーク１０を介してユーザ端末１１、認証局サーバ１５、サービスサーバ１７等との間でデータ通信を行うためのものである。

【００２５】認証局サーバ１５は、電子証明書の発行要求に応じて、受信した署名対象の情報に電子署名を施す等して電子証明書を生成・発行する。

【００２６】サービスサーバ１７は、例えば図５に示すように、制御部１７１と、記憶部１７２と、通信制御部１７３と、を備えるコンピュータ等から構成される。

【００２７】制御部１７１は、記憶部１７２に記憶される動作プログラム等を実行することにより、アクセス管理部１７１ａ、要求処理部１７１ｂ、サービス提供部１７１ｃ、暗号処理部１７１ｄ等を論理的に実現する。アクセス管理部１７１ａは、認証管理サーバ１３からのログイン要求に応じて、提示されたペルソナＩＤ（電子証明書）を照合することにより、サービス要求元のユーザを確認する処理等を行う。要求処理部１７１ｂは、認証管理サーバ１３からの要求を受け付けてサービス提供部１７１ｃに受け渡し、また、サービス提供部１７１ｃから処理結果を受け取って認証管理サーバ１３に供給する処理等を行う。サービス提供部１７１ｃは、サービス提供のための処理を行う。暗号処理部１７１ｄは、電子署名の確認処理やデータの暗号化／復号化処理等を行う。

【００２８】記憶部１７２は、制御部１７１が実行する動作プログラムや、処理に必要な各種のデータを記憶する。また、記憶部１７２は、登録ユーザのペルソナＩＤ等を登録情報として記憶する。通信制御部１７３は、ネットワーク１０を介して認証管理サーバ１３等との間でデータ通信を行うためのものである。

【００２９】以下に、この実施の形態に係るユーザ認証システムの動作について本発明の特徴部分を中心に説明する。

【００３０】初めに、ユーザが認証管理サーバ１３にユーザ登録する場合の処理について図６を参照して説明する。まず、ユーザは認証管理サーバ１３へのユーザ登録に使用する電子証明書（プライマリＩＤ）を取得するため、ユーザ端末１１を操作して、認証局サーバ１５に対して電子証明書の発行を要求する（Ｌ１１）。認証局サーバ１５は、ユーザ端末１１からの証明書の発行要求に応じて、ユーザの電子証明書を生成し（Ｌ１２）、要求元のユーザ端末１１に供給する（Ｌ１３）。ユーザ端末１１は、発行された電子証明書をＩＣカード等に格納する（Ｌ１４）。

【００３１】次に、ユーザ端末１１は、ユーザの操作に応じて、認証管理サーバ１３に対してユーザ登録要求を送信する（Ｌ１５）。これに応じて、認証管理サーバ１３は、所定のユーザ登録処理を行う（Ｌ１６）。このユーザ登録処理では、例えば、ユーザ端末１１にプライマリＩＤを要求して、ＩＣカード等に格納されたプライマリＩＤを取得し、取得したプライマリＩＤについて、電子署名を確認等する。そして、証明書の正当性が確認されると、プライマリＩＤや、プライマリＩＤに含まれるユーザの個人情報（メイン情報、付属情報）等をユーザＤＢ１３２ａに記憶して、登録結果をユーザ端末１１に返信し（Ｌ１７）、ユーザ登録処理を終了する。

【００３２】次に、サービス利用の際にサービスサーバ１７に提示する電子証明書（ペルソナＩＤ）を発行する処理について図７を参照して説明する。例えばユーザ端末１１は、ユーザの操作に応じて、認証管理サーバ１３に対して電子証明書（ペルソナＩＤ）の発行要求を送信する（Ｌ２１）。これに応じて、認証管理サーバ１３は、証明書の内容情報を入力させる登録画面をユーザ端末１１に供給する（Ｌ２２）。ユーザ端末１１は、認証管理サーバ１３からの登録画面を表示して、ユーザによる証明書の内容情報の入力を受けて、入力された情報を認証管理サーバ１３に送信する（Ｌ２３）。

【００３３】認証管理サーバ１３は、ユーザ端末１１からの入力データの内容をチェックし、新規にキーペア（秘密鍵と公開鍵）を作成し、入力内容及び作成したキーの片方（公開鍵）を含む証明書のリクエストを生成して（Ｌ２４）、認証局サーバ１５に送信する（Ｌ２５）。認証局サーバ１５は、認証管理サーバ１３から受信した要求内容をチェックした後、署名対象データに署名を施す等して、電子証明書（ペルソナＩＤ）を作成し（Ｌ２６）、認証管理サーバ１３に送信する（Ｌ２７）。認証管理サーバ１３は、受信したペルソナＩＤをユーザＤＢ１３２ａに登録するとともに（Ｌ２８）、ペルソナＩＤの発行が完了したことを示す通知画面をユーザ端末１１に供給する（Ｌ２９）。

【００３４】次に、ユーザが利用したいサービスについて認証管理サーバ１３がアカウント登録する場合の処理について図８、図９を参照して説明する。例えば、ユーザがユーザ端末１１に表示された所定の操作画面におけるログインボタンを押下すると、ユーザ端末１１はＰＩＮ（Personal Identification Number）入力を要求して、ＰＩＮ入力を受け付ける。そして、入力されたＰＩＮを照合することによりユーザの確認を行った後、ＩＣカードからプライマリＩＤを読み込み（Ｌ３１）、認証管理サーバ１３にログイン要求を送信する（Ｌ３２）。認証管理サーバ１３は、ログイン要求に応答して、プライマリＩＤを用いてユーザの確認を行い、ユーザ端末１１との通信で使うセッションキーを生成し（Ｌ３３）、ログイン結果とともにユーザ端末１１に供給する（Ｌ３４）。ユーザ端末１１は、受信したセッションキーを保持するとともに、ログイン結果を表示する（Ｌ３５）。

【００３５】次に、ユーザは新規サービスの登録を要求する旨を入力し、これに応じて、ユーザ端末１１は、サービスの登録要求を認証管理サーバ１３に送信する（Ｌ３６）。認証管理サーバ１３は、サービスの登録要求に応じて、要求されたサービスに対応するサービスサーバ１７に対して、アカウント登録に必要な情報を問い合わせる（Ｌ３７）。サービスサーバ１７は、認証管理サーバ１３からの問い合わせに応じて、アカウント登録に必要なユーザ情報の項目（登録必要項目）の情報を認証管理サーバ１３に送信する（Ｌ３８）。これに応答して、認証管理サーバ１３は、要求元のユーザについて記憶部１３２に登録されているペルソナＩＤを参照し、それぞれに含まれているユーザ情報のデータ項目と、サービスサーバ１７から取得した登録必要項目と、を比較して、適合するペルソナＩＤがあるかを判別する（Ｌ３９）。

【００３６】この判別において、適合するペルソナＩＤがある場合、認証管理サーバ１３は、該当するペルソナＩＤを抽出し、抽出結果をユーザ端末１１に供給して（Ｌ４０）、使用対象のペルソナＩＤをユーザに選択させる（Ｌ４１）。そして、選択されたペルソナＩＤを含むアカウント登録要求をサービスサーバ１７に送信する（Ｌ４２）。これに応じて、サービスサーバ１７はアカウント登録処理を行う（Ｌ４３）。なお、適合するペルソナＩＤの情報をユーザ端末１１に供給した際に、それらを使用しない旨の入力があった場合には、認証管理サーバ１３は、例えば、ユーザ端末１１に要求して、必要な情報をユーザに入力させ、入力データに基づくペルソナＩＤの発行を受け、そのペルソナＩＤを用いてアカウント登録する。

【００３７】また、適合するペルソナＩＤがない場合、認証管理サーバ１３は、例えば不足情報の入力画面をユーザ端末１１に供給する等して（Ｌ４４）、アカウント登録に必要な情報をユーザ端末１１から取得する（Ｌ４５）。そして、取得した情報に基づく新たなペルソナＩ

Ｄの発行を認証局サーバ１５に要求し（Ｌ４６）、ペルソナＩＤの発行を受ける（Ｌ４７）。そして、認証管理サーバ１３は、新たに発行されたペルソナＩＤを含むアカウント登録要求をサービスサーバ１７に送信する（Ｌ４８）。これに応じて、サービスサーバ１７は、アカウント登録処理を行う（Ｌ４９）。

【００３８】ここで、上述したサービス側へのアカウント登録処理における認証管理サーバ１３の動作の詳細を図１０のフローチャートを参照して説明する。まず、認証管理サーバ１３の制御部１３１は、サービスの登録要求に応じて、要求されたサービスに対応するサービスサーバ１７にアクセスし、アカウント登録に必要な情報を問い合わせて取得する（ステップＳ１１）。次に、制御部１３１は、要求元のユーザについて記憶部１３２に登録されているペルソナＩＤを参照し、それぞれに含まれているユーザ情報のデータ項目と、サービスサーバ１７から取得した登録必要項目と、を比較して（ステップＳ１２）、既存のペルソナＩＤのデータ項目が登録必要項目を満たす場合には（ステップＳ１３）、該当するペルソナＩＤを抽出し、使用対象の候補のペルソナＩＤの情報としてユーザ端末１１に供給して表示させる（ステップＳ１４）。

【００３９】そして、ユーザ端末１１から、候補のペルソナＩＤのいずれかが選択された旨の情報を受信した場合（ステップＳ１５）、制御部１３１は、選択されたペルソナＩＤを用いてサービスサーバ１７へアカウント登録要求を送信して、アカウント登録を受ける（ステップＳ１６）。

【００４０】また、ユーザ端末１１から、候補のペルソナＩＤが選択されなかった旨の情報を受信した場合には（ステップＳ１５）、制御部１３１は、アカウント登録に必要な情報の入力画面を供給する等して所定のユーザ情報をユーザ端末１１から取得し、取得した情報に基づく電子証明書の発行を認証局サーバ１５に要求して、新たな電子証明書（ペルソナＩＤ）の発行を受ける（ステップＳ１７）。そして、発行された電子証明書（ペルソナＩＤ）を用いてサービスサーバ１７へアカウント登録要求を送信して、アカウント登録を受ける（ステップＳ１６）。

【００４１】また、ステップＳ１３において、既存のペルソナＩＤのデータ項目よりも、登録必要項目の方が多い場合には、アカウント登録に必要な情報をユーザ端末１１から取得し、取得した情報に基づく電子証明書の発行を認証局サーバ１５に要求して、新たな電子証明書（ペルソナＩＤ）の発行を受ける（ステップＳ１７）。そして、発行された電子証明書（ペルソナＩＤ）を用いてサービスサーバ１７へアカウント登録要求を送信して、アカウント登録を受ける（ステップＳ１６）。

【００４２】次に、ユーザがサービスを利用する場合の処理について説明する。まず、ユーザがサービス提供側のユーザ認証を受けるまでの処理について図１１、図１２を参照して説明する。まず、上記のアカウント登録処理の場合と同様に、ユーザがユーザ端末１１を用いて認証管理サーバ１３にログインする（Ｌ５１～Ｌ５５）。次に、ユーザはペルソナＩＤの一覧（ペルソナリスト）を要求する旨をユーザ端末１１に入力し、これに応じて、ユーザ端末１１は、ユーザのペルソナリストを認証管理サーバ１３に要求する（Ｌ５６）。認証管理サーバ１３は、ペルソナリストの要求に応じて、そのユーザについて登録されているペルソナＩＤをユーザＤＢ１３２ａから読み出し、ペルソナリストを生成してユーザ端末１１に供給して表示させる（Ｌ５７、Ｌ５８）。ユーザ端末１１は、表示されたペルソナリストから、使用するペルソナＩＤの選択入力を受け付け、選択されたペルソナＩＤを認証管理サーバ１３に通知する（Ｌ５９）。

【００４３】次に、認証管理サーバ１３は、ユーザＤＢ１３２ａを参照して、ユーザにより選択されたペルソナＩＤでユーザ登録がされているサービスを抽出し、抽出されたサービス一覧をユーザ端末１１に供給して表示させる（Ｌ６０、Ｌ６１）。ユーザ端末１１は、表示されたサービス一覧から、利用するサービスをユーザに選択入力させ、選択されたサービスを認証管理サーバ１３に通知する（Ｌ６２）。認証管理サーバ１３は、選択されたサービスに対応するサービスサーバ１７を特定し、ユーザに選択されたペルソナＩＤを含むログイン要求を送信する（Ｌ６３）。サービスサーバ１７は、認証管理サーバ１３からログイン要求に応じて、受信したペルソナＩＤを照合することによりユーザ確認を行い、認証管理サーバ１３との通信で使うセッションキーを生成し（Ｌ６４）、ログイン結果とともに認証管理サーバ１３に供給する（Ｌ６５）。認証管理サーバ１３は、サービスサーバ１７から受信したセッションキーを保持し、ログイン結果をユーザ端末１１に通知する（Ｌ６６）。

【００４４】次に、サービス提供側のユーザ認証の完了後、実際にサービスを受ける場面の処理について、銀行の融資相談窓口のサービスを利用する場合を例に図１３を参照して説明する。例えば、ユーザはユーザ端末１１に相談内容を入力すると、ユーザ端末１１は、ユーザ端末１１と認証管理サーバ１３とのセッションキーで入力データを暗号化して認証管理サーバ１３へ送信する（Ｌ７１）。認証管理サーバ１３は、ユーザ端末１１からの受信データを、ユーザ端末１１と認証管理サーバ１３とのセッションキーで復号化した後（Ｌ７２）、認証管理サーバ１３とサービスサーバ１７とのセッションキーで暗号化してサービスサーバ１７へ送信する（Ｌ７３）。

【００４５】サービスサーバ１７は、認証管理サーバ１３からの受信データを、認証管理サーバ１３とサービスサーバ１７とのセッションキーで復号化し、処理に必要な情報（融資相談内容）を抽出する（Ｌ７４）。そして、抽出された情報に基づいて、サービス提供側の担当

者が融資相談に対する返答等をサービスサーバ１７へ入力する（Ｌ７５）。サービスサーバ１７は、入力されたデータ認証管理サーバ１３とサービスサーバ１７とのセッションキーで暗号化して認証管理サーバ１３に送信する（Ｌ７６）。

【００４６】認証管理サーバ１３は、サービスサーバ１７からの受信データを、認証管理サーバ１３とサービスサーバ１７とのセッションキーで復号化した後（Ｌ７７）、ユーザ端末１１と認証管理サーバ１３との間のセッションキーで暗号化してユーザ端末１１に送信する（Ｌ７８）。ユーザ端末１１は、認証管理サーバ１３からの受信データを、ユーザ端末１１と認証管理サーバ１３とのセッションキーで復号化し（Ｌ７９）、融資相談に対する返答を示す情報を表示する。

【００４７】以上説明したように、本発明によれば、アカウント登録のために各種サービスへ開示するユーザ情報の内容をユーザ自身がサービス毎に指定することができるため、自己の情報の開示をユーザ自身がコントロールすることができ、ユーザのプライバシーを保護することができる。また、各サービスへの登録や、各サービスに提示する電子証明書の取得・管理を認証管理サーバ１３が行うことにより、ユーザの負荷が軽減され、システムの利便性を向上することができる。また、仮にユーザがサービス側に本当の情報を開示していなくとも、認証管理サーバ１３において身元確認がなされているため、各サービス側は安心してサービスを提供することができる。

【００４８】なお、上記説明におけるプライマリＩＤ、ペルソナＩＤの構成内容は一例であり、これに限定されない。また、上記説明では、ユーザのプライマリＩＤ、秘密鍵、公開鍵等をＩＣカードなどの情報記憶媒体に記憶するようにしているが、これに限定されず、例えば、ユーザ端末１１の記憶部に記憶するようにしてもよい。

【００４９】また、各装置やＤＢの構成は、任意に変更可能である。また、各サーバは、協働して動作する複数台のコンピュータシステムから構成されてもよく、各サーバの機能を１台のコンピュータシステムで統合して実現してもよい。

【００５０】なお、この発明のシステムは、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、上述の動作を実行するためのプログラムをコンピュータ読み取り可能な記録媒体（ＦＤ、ＣＤ－ＲＯＭ、ＤＶＤ等）に格納して配布し、該プログラムをコンピュータにインストールすることにより、上述の処理を実行する各サーバ等を構成してもよい。また、インターネット等のネットワーク上のサーバ装置が有するディスク装置に格納しておき、例えば搬送波に重畳してコンピュータにダウンロード等するようにしてもよい。また、上述の機能を、ＯＳが分担又はＯＳとアプリケーションの共同により実現する場合等には、ＯＳ以外の部分のみを媒体に格納して配布してもよく、また、搬送波に重畳してコンピュータにダウンロード等してもよい。

【００５１】

【発明の効果】この発明によれば、アカウント登録のために開示するユーザ情報の内容をユーザ自身がコントロールすることができるため、ユーザのプライバシーを保護することができる。

【図面の簡単な説明】

【図１】この発明の実施の形態に係るユーザ認証システムの構成を示す図である。

【図２】プライマリＩＤの構成の一例を示す図である。

【図３】図１のユーザ認証システムで使用される認証管理サーバの構成を示す図である。

【図４】ペルソナＩＤの構成の一例を示す図である。

【図５】図１のユーザ認証システムで使用されるサービスサーバの構成を示す図である。

【図６】ユーザが認証管理サーバにユーザ登録する場合の処理を説明するための図である。

【図７】サービスサーバに提示する電子証明書（ペルソナＩＤ）を発行する処理を説明するための図である。

【図８】サービスサーバへアカウント登録する場合の処理を説明するための図である。

【図９】サービスサーバへアカウント登録する場合の処理を説明するための図である。

【図１０】アカウント登録処理における認証管理サーバの動作を説明するためのフローチャートである。

【図１１】ユーザがサービス提供側のユーザ認証を受けるまでの処理を説明するための図である。

【図１２】ユーザがサービス提供側のユーザ認証を受けるまでの処理を説明するための図である。

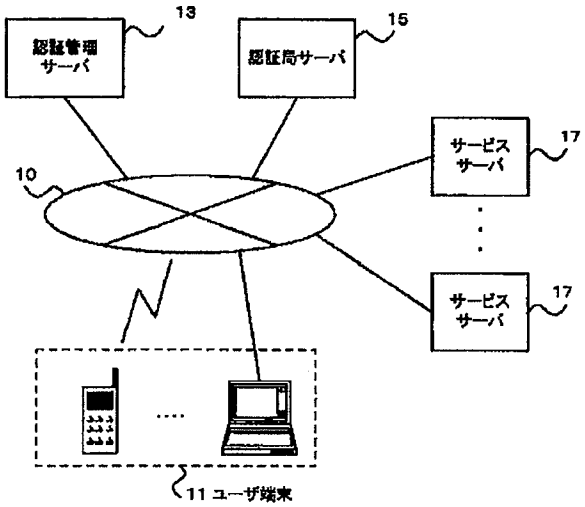
【図１３】サービス提供側のユーザ認証の完了後、実際にサービスを受ける場面の処理を説明するための図である。

【符号の説明】

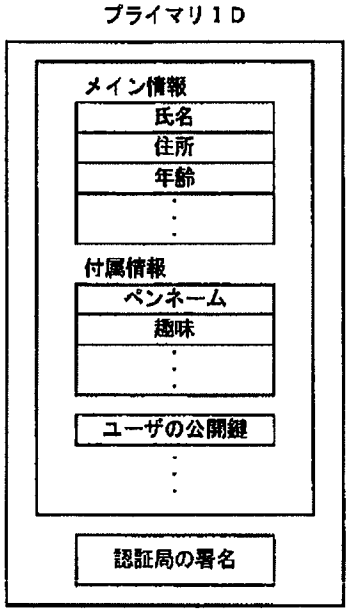
１０	ネットワーク
１１	ユーザ端末
１３	認証管理サーバ
１５	認証局サーバ
１７	サーピスサーバ
１３１、１７１	制御部
１３２、１７２	記憶部
１３３、１７３	通信制御部
１３１ａ	要求処理部
１３１ｂ	ユーザ認証部
１３１ｃ	証明書管理部
１３１ｄ	サービスＩＦ部
１３１ｅ	セッション管理部
１３１ｆ	暗号処理部
１３２ａ	ユーザＤＢ

１７１ａ　アクセス管理部
１７１ｂ　要求処理部
１７１ｃ　サービス提供部
１７１ｄ　暗号処理部

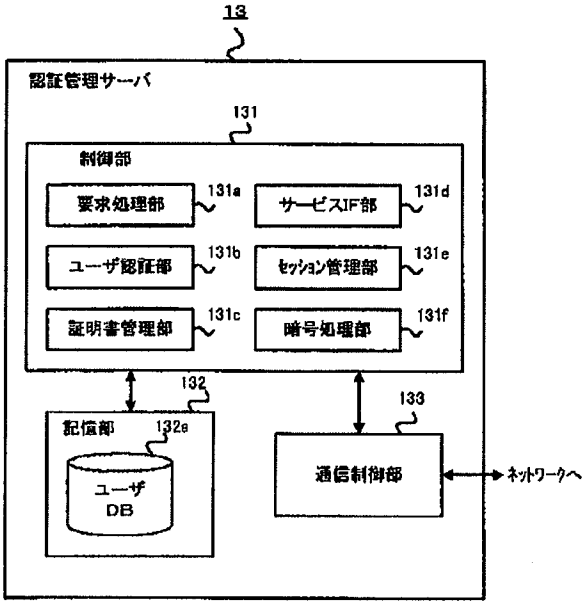
【図１】



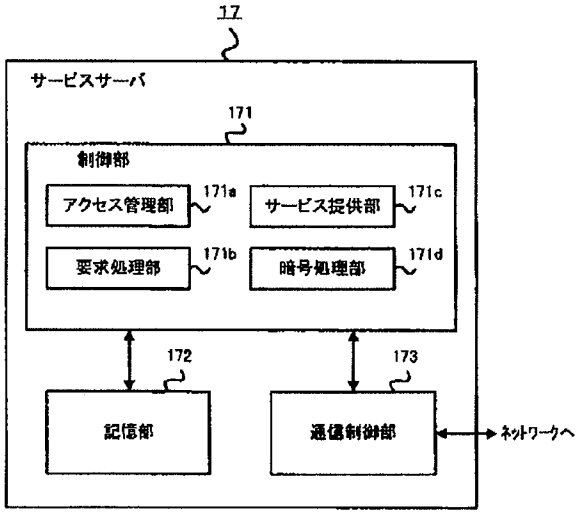
【図２】



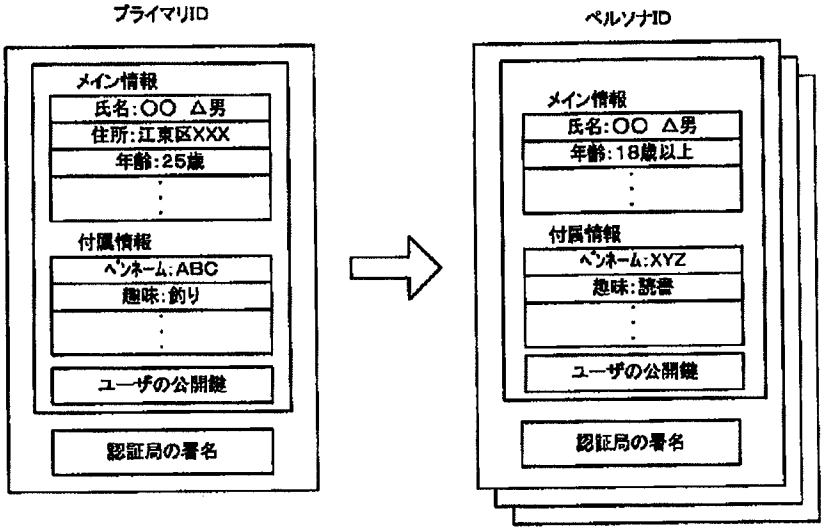
【図３】



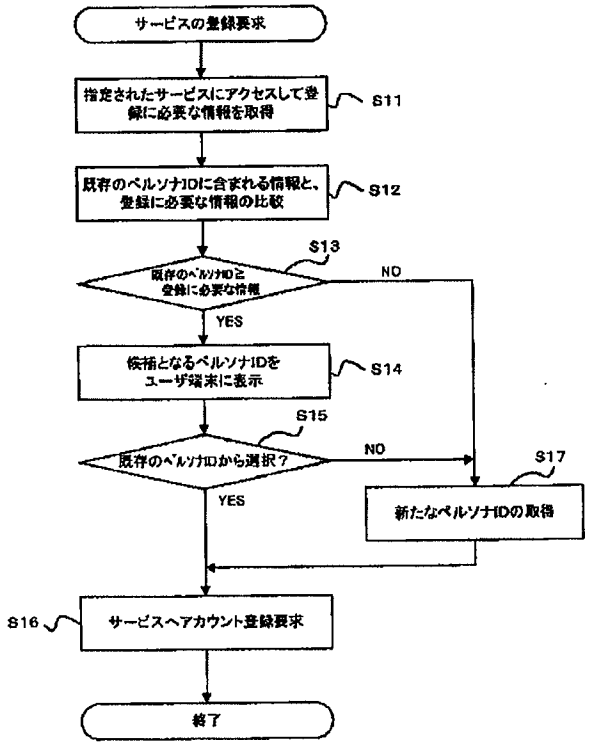
【図５】



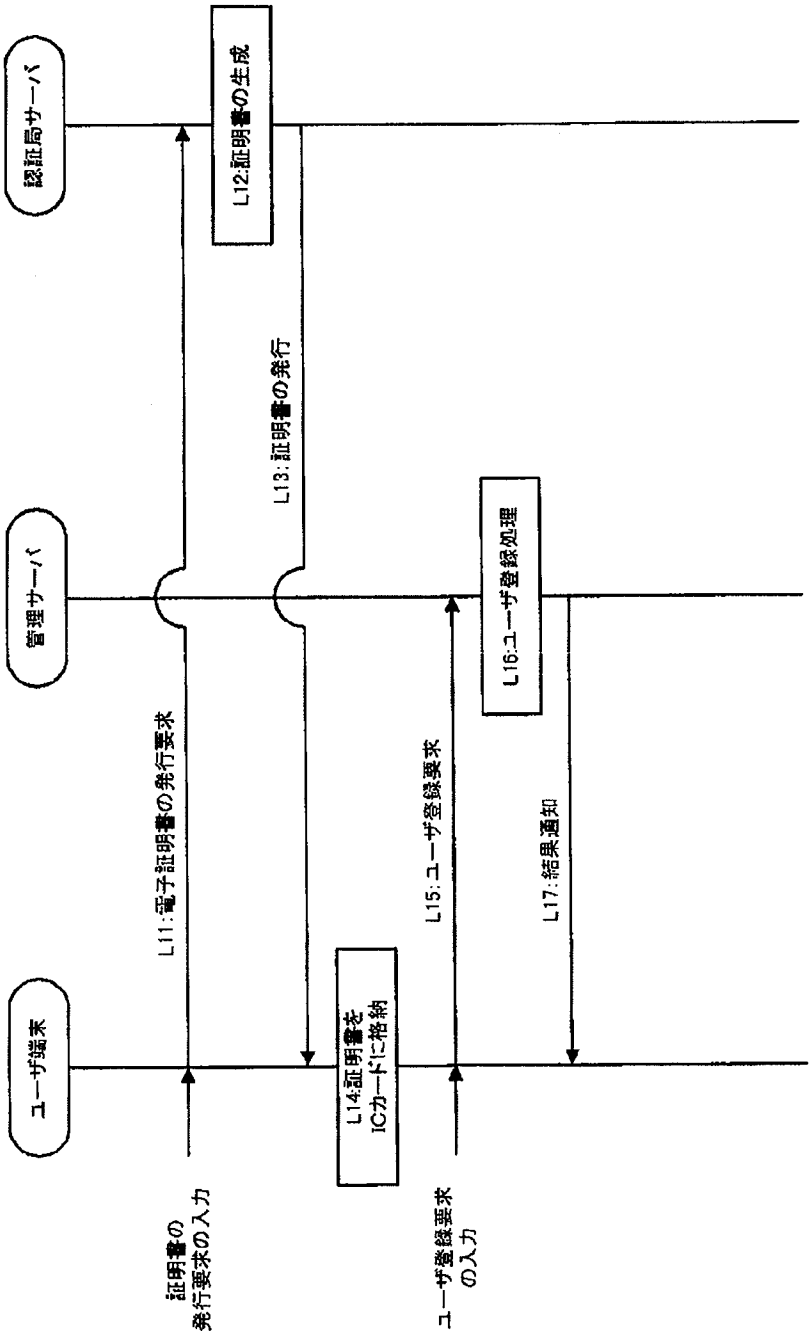
【図４】


プライマリID
メイン情報
氏名:○○ △男
住所:江東区XXX
年齢:25歳
付属情報
ペンネーム:ABC
趣味:釣り
ユーザの公開鍵
認証局の署名
ペルソナID
メイン情報
氏名:○○ △男
年齢:18歳以上
付属情報
ペンネーム:XYZ
趣味:読書
ユーザの公開鍵
認証局の署名

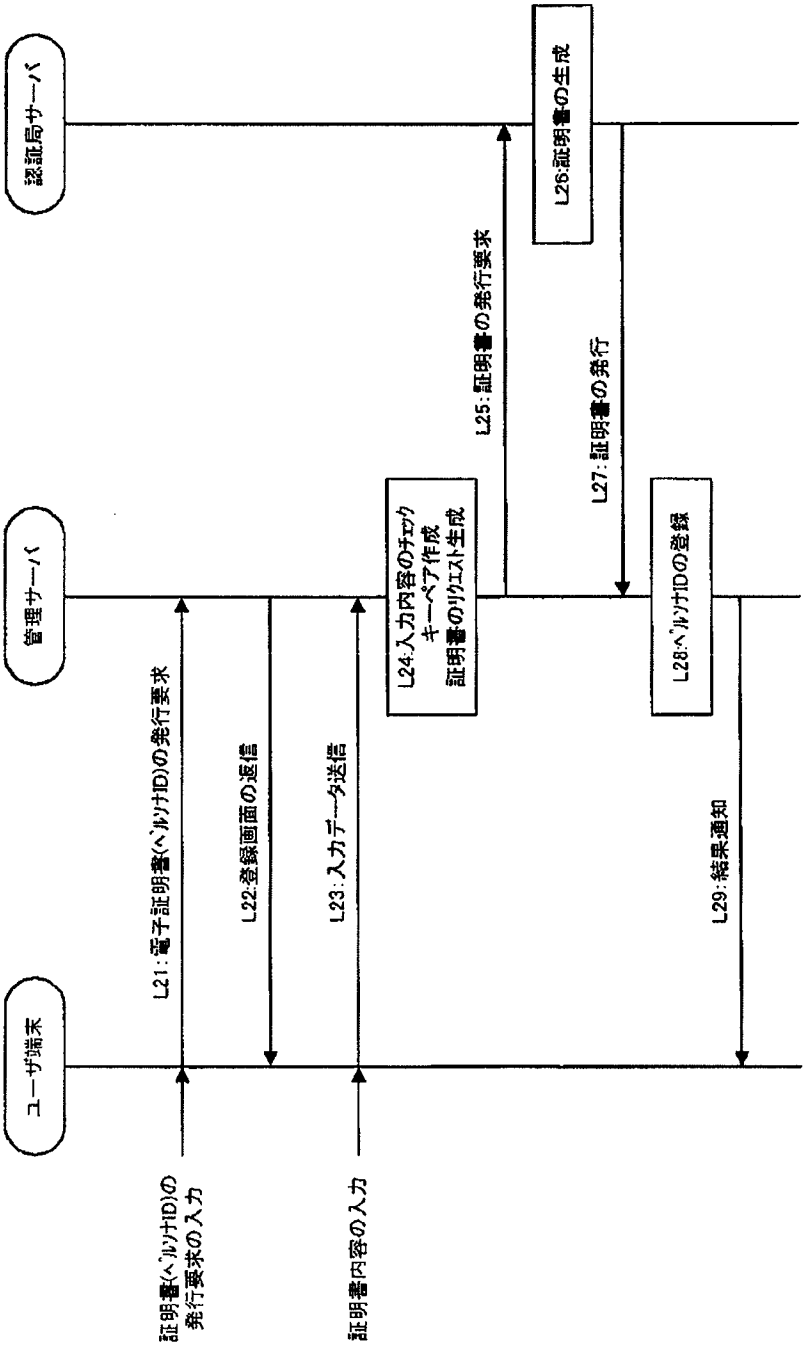
【図１０】


サービスの登録要求
指定されたサービスにアクセスして登録に必要な情報を取得
S11
既存のペルソナIDに含まれる情報と、登録に必要な情報の比較
S12
S13
既存のペルソナIDと登録に必要な情報
NO
YES
候補となるペルソナIDをユーザ端末に表示
S14
S15
既存のペルソナIDから選択？
NO
S17
YES
新たなペルソナIDの取得
S16
サービスへアカウント登録要求
終了

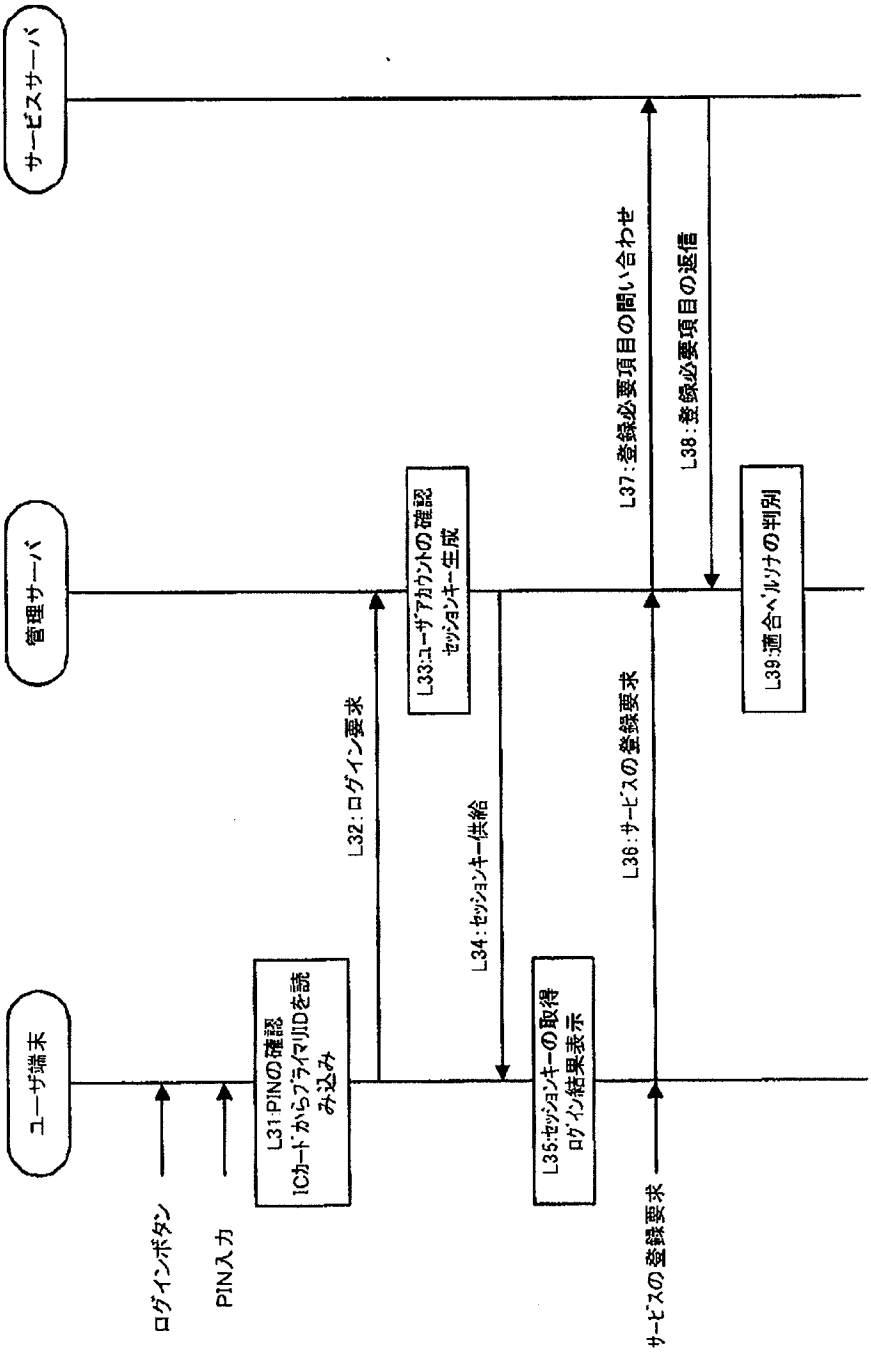
【図6】


認証局サーバ
管理サーバ
ユーザ端末
L12:証明書の生成
L11:電子証明書の発行要求
L13:証明書の発行
L16:ユーザ登録処理
L15:ユーザ登録要求
L17:結果通知
L14:証明書をICカードに格納
証明書の発行要求の入力
ユーザ登録要求の入力

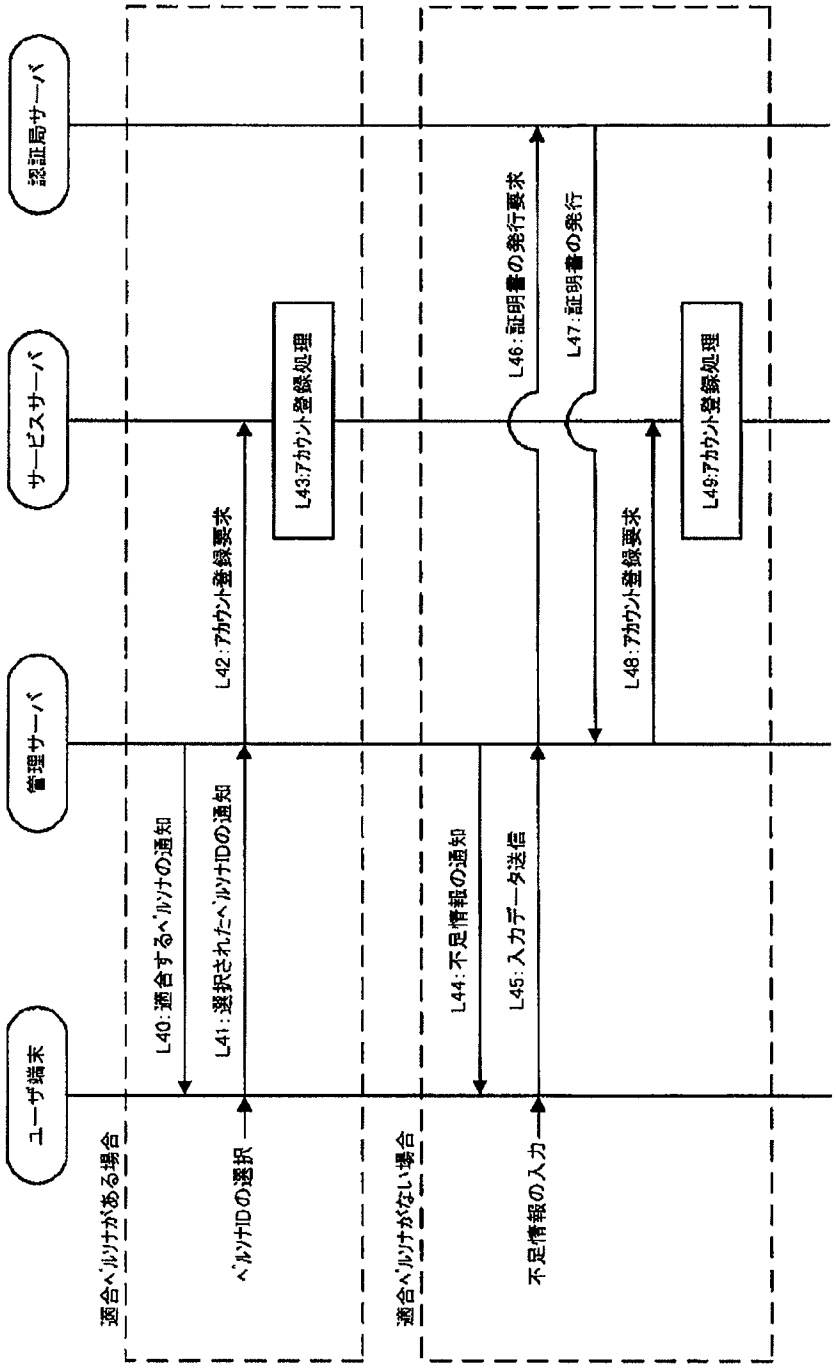
【図7】


ユーザ端末
管理サーバ
認証局サーバ
証明書(ペルソナID)の発行要求の入力
証明書内容の入力
L21:電子証明書(ペルソナID)の発行要求
L22:登録画面の返信
L23:入力データ送信
L24:入力内容のチェック
キーペア作成
証明書のリクエスト生成
L25:証明書の発行要求
L26:証明書の生成
L27:証明書の発行
L28:ペルソナIDの登録
L29:結果通知

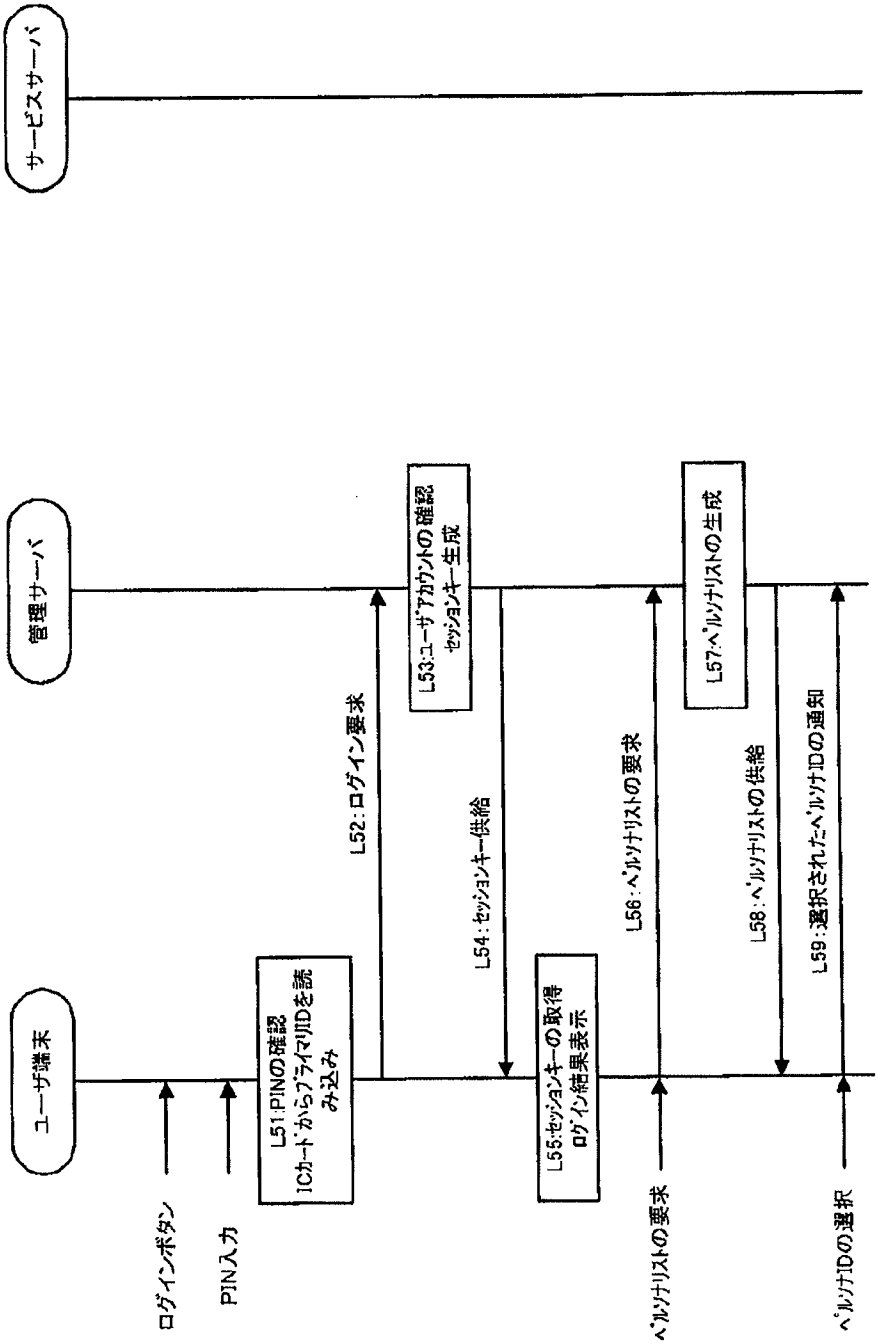
【図8】


ユーザ端末
管理サーバ
サービスサーバ
ログインボタン
PIN入力
L31:PINの確認
ICカードからプライマリIDを読み込み
L32:ログイン要求
L33:ユーザアカウントの確認
セッションキー生成
L34:セッションキー供給
L35:セッションキーの取得
ログイン結果表示
サービスの登録要求
L36:サービスの登録要求
L37:登録必要項目の問い合わせ
L38:登録必要項目の返信
L39:適合ペルソナの判別

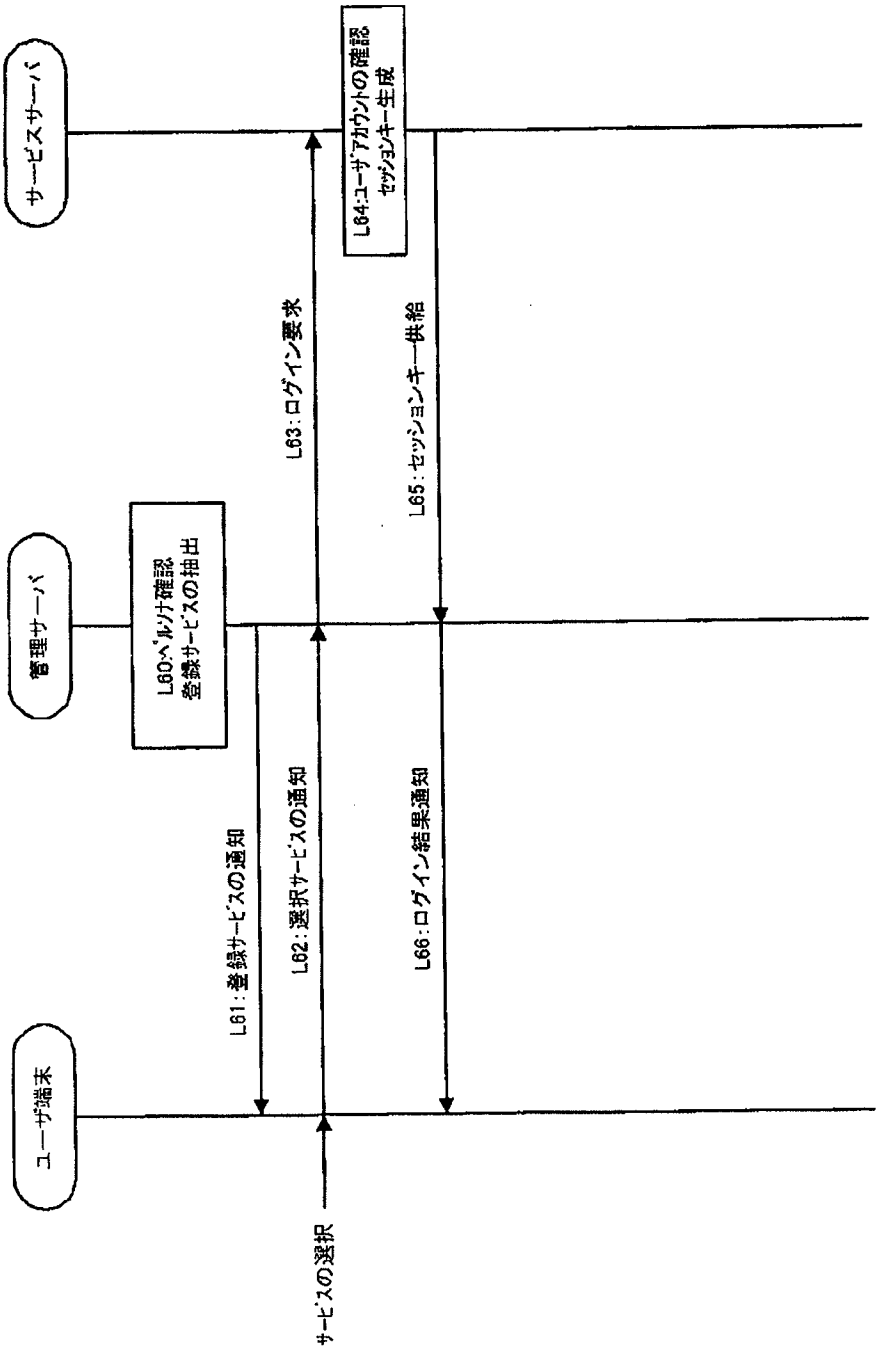
【図９】


ユーザ端末
管理サーバ
サービスサーバ
認証局サーバ
適合ﾍﾞﾙｿﾅがある場合
L40:適合するﾍﾞﾙｿﾅの通知
L41:選択されたﾍﾞﾙｿﾅIDの通知
L42:アカウント登録要求
L43:アカウント登録処理
ﾍﾞﾙｿﾅIDの選択
適合ﾍﾞﾙｿﾅがない場合
L44:不足情報の通知
L45:入力データ送信
L46:証明書の発行要求
L47:証明書の発行
L48:アカウント登録要求
L49:アカウント登録処理
不足情報の入力

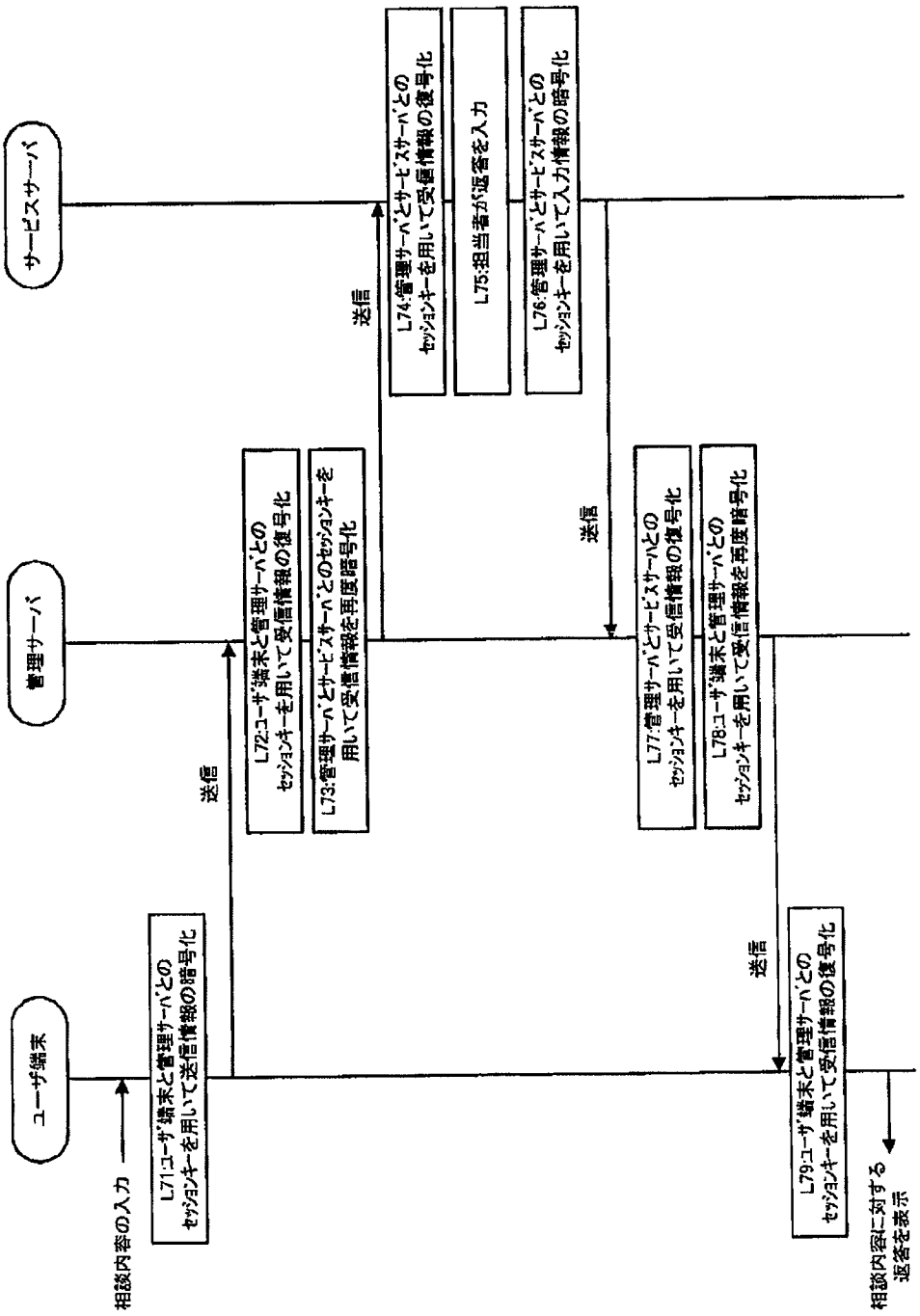
【図１１】


ユーザ端末
管理サーバ
サービスサーバ
ログインボタン
PIN入力
L51:PINの確認
ICカードからプライマリIDを読み込み
L52:ログイン要求
L53:ユーザアカウントの確認
セッションキー生成
L54:セッションキー供給
L55:セッションキーの取得
ログイン結果表示
ペルソナリストの要求
L56:ペルソナリストの要求
L57:ペルソナリストの生成
L58:ペルソナリストの供給
ペルソナIDの選択
L59:選択されたペルソナIDの通知

【図12】


サービスサーバ
管理サーバ
ユーザ端末
L60:ペルソナ確認
登録サービスの抽出
L61:登録サービスの通知
L62:選択サービスの通知
L63:ログイン要求
L64:ユーザアカウントの確認
セッションキー生成
L65:セッションキー供給
L66:ログイン結果通知
サービスの選択

【図１３】



フロントページの続き

(72)発明者　楠田　哲也
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

(72)発明者　宮田　功治
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

(72)発明者 横山 重俊
東京都江東区豊洲三丁目３番３号 株式会
社エヌ・ティ・ティ・データ内

Ｆターム(参考) 5B085 AA08 AE02 AE09 AE23 BA07
BG02 BG07
5J104 MA01